Organization TC2800 Bldg./Room Jeff
U. S. DEPARTMENT OF COMMERCE
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
IF UNDELIVERABLE RETURN IN TEN DAYS

OFFICIAL BUSINESS

U.S. OFFICIAL MAIL
PENALTY FOR
PRIVATE USE $300
PITNEY BOWES
02 1A
0004205065
$ 01.11⁰
AUG 08 2006
MAILED FROM ZIP CODE 22314

AN EQUAL OPPORTUNITY EMPLOYER

REASON CHECKED
- ☐ Moved, Left No Address
- ☐ Forwarding Order Expired
- ☐ Unable To Forward
- ☐ Attempted - Not Known
- ☐ Unclaimed
- ☐ No Such Street
- ☐ Refused
- ☐ Insufficient Address
- ☐ No Such Number

- ☐ INSUFFICIENT ADDRESS
- ☒ ATTEMPTED NOT KNOWN
- ☐ NO SUCH NUMBER/ STREET
- ☐ NOT DELIVERABLE AS ADDRESSED - UNABLE TO FORWARD
- ☐ OTHER

RTS
RETURN TO SENDER

RECEIVED
AUG 18 2006
USPTO MAIL CENTER

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/709,751	05/26/2004	Fonda J. Daniels	014682.000007	3750

44870 7590 08/08/2006

MOORE & VAN ALLEN, PLLC
P.O. Box 13706
Research Triangle Park, NC 27709

EXAMINER
SANDERS, AARON J

ART UNIT	PAPER NUMBER
2191	

DATE MAILED: 08/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/709,751	DANIELS ET AL.	
	Examiner	Art Unit	
	Aaron J. Sanders	2191	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 May 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 May 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2 September 2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The disclosure is objected to because the font size is too large for comfortable reading. While the MPEP does not specify a maximum font size, it suggests that nonscript type fonts (e.g. Arial, Times New Roman, or Courier) have a font size of 12. See MPEP 608.01. Appropriate correction is required.

Claim Objections

Claim 13 is objected to for the following informality: the phrase 'distributing original content object' is grammatically incorrect. Appropriate correction is required.

Claim 27 is objected to for the following informality: in the phrase 'in responsive to the request', 'responsive' is incorrect. Appropriate correction is required.

Claim 39 is objected to for the following informality: 'sevlet' is misspelled. Appropriate correction is required.

Claim 42 is objected to for the following informality: a transition phrase is required between 'the method of claim 40,' and 'deleting or replacing'. Appropriate correction is required.

Claims 3, 5, 11, 22, 28, 36, and 45 are objected to because of the following informalities: the term 'xLink' is undefined. XLink is a W3C specification, and is therefor subject to change. The term may be used in the applicant's claims, but it must be accompanied by generic language. Appropriate correction is required.

Claims 7, 18, 30, 31, 36, 38, and 39 are objected to because of the following informalities: the term 'servlet' is undefined. A servlet is an application programming interface (API) object in Java, and is therefor subject to change. The term may be used in the applicant's claims, but it must be accompanied by generic language. Appropriate correction is required.

Claims 8, 19, 28-31, and 36-39 are objected to because of the following informalities: the term 'P3P servlet' is undefined. P3P is a W3C protocol, and is therefor subject to change. The term may be used in the applicant's claims, but it must be accompanied by generic language. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 2, 4, 6, 8-10, 12, 13, 15, 16, 19-21, 23, 24, 27, 32, 33, 35, 40, 41, 43, and 44 are rejected under 35 U.S.C. 102(b) as being anticipated by Bohrer et al.

As per claims 1, 2, 4, 6, 8-10, 12, 13, 15, 16, 19-21, 23, 24, 27, 32, 33, 35, 40, 41, 43, and 44, Bohrer et al. teach:

1. A method for managing privacy preferences or access to restricted information, comprising:

tagging restricted or personal information (See e.g. [0031], 'the Data Subject can use a web browser to set up one or more privacy policies by specifying authorization rules describing to whom, and under what conditions, the data can be released via communication links'); and

defining a content object with a link to the restricted or personal information (See e.g. [0017], 'it allows a data subject to express privacy preference policies for controlling access to their personal data that is distributed across multiple enterprises and repositories' where 'personal data' is the 'content object' and 'express privacy preference policies' is the 'link').

2. The method of claim 1, wherein defining the content object comprises defining the content object as a web document or a mark-up language file (See e.g. [0029], 'The invention involves information that is communicated between computers; this information could be in hypertext markup language (HTML), or extensible markup language (XML)').

4. The method of claim 1, further comprising:

storing the content object (See e.g. [0017], 'it allows a data subject to express complex policies on a large set of personal data in a way that is applicable regardless of the specific representation and data model used by enterprises that store that data'); and

providing access to the content object (See e.g. [0017], 'it allows a data subject to specify complex privacy preferences that include who can access the data').

6. The method of claim 1, further comprising:

receiving a request for information (See e.g. [0032], 'a Data Requester 105 can use a web browser 106 or some other computer programs 107 to send requests for data');

interrogating content sources (See e.g. [0035], 'The Profile Responder 116 receives requests for profile information... and uses the Policy authorization engine to check the authorization and privacy policies'); and

collecting any content objects responsive to the request (See e.g. [0016], 'The data is released only if the privacy declaration of the requester matches the constraints imposed by the data subject via its privacy preferences').

8. The method of claim 6, further comprising distributing any content object responsive to the request to a P3P servlet (See e.g. [0049], 'The Privacy Preference 302 specifies why and how the data can be accessed in terms of the P3P standards').

9. The method of claim 6, further comprising distributing any content object responsive to the request to a privacy function (See e.g. [0030], 'This embodiment supports the enforcement of privacy preferences in data exchanges according to authorization checks based on the privacy preferences specified by a data subject with the privacy policies of a data requester' where the 'authorization checks' are considered 'privacy functions').

10. The method of claim 9, further comprising parsing privacy preferences of an author of the content object or other restriction preferences (See e.g. [0033], 'the system must provide several different functionalities, including the ability to... authorize release of data based on authorization rules and privacy policy matching and release data').

12. The method of claim of claim 9, further comprising comparing the privacy content object or other preferences of an author of the restriction preferences to a content provider's policies (See e.g. [0003], 'In some cases the web site's privacy policy is compared to the consumer's policy preferences and warnings are issued when there is a mismatch').

13. The method of claim 12, further comprising distributing original content object to a requester in response to the privacy preferences of the author of the content object or other restriction preferences being consistent with the content provider's policies (See e.g. [0017], 'an independent third party acting as a data-subject's personal data service and providing various services including... matching privacy policies, gathering data from third parties and releasing and/or authorizing release of data to data requesters').

15. A method for managing privacy or access to restricted information, comprising:

collecting a content object responsive to a request (See e.g. [0032], 'a Data Requester 105 can use a web browser 106 or some other computer programs 107 to send requests for data 109 as well as receive replies 110 to that request along with any returned data');

accessing privacy preferences of an author of the content object or other restriction preferences (See e.g. [0033], 'the system must provide several different functionalities, including the ability to... define authorization rules and privacy controls'); and

comparing the privacy preferences or other restriction preferences to a content provider's policies (See e.g. [0033], 'the system must provide several different functionalities, including the ability to... authenticate requesters, authorize release of data based on authorization rules and privacy policy matching' where [0013], 'a data subject may want to setup privacy preference policies which can allow fully automatic release of data, even without knowing about the requester or the request itself... Similarly, a data subject may allow access to certain, non-identifiable financial data such as employment status and salary range, thus enabling interested financial institutions to automatically access such data and send solicitations for credit cards/loan requests to the data subjects' indicates that a 'requester' can also be a 'content provider').

16. The method of claim 15, further comprising distributing the content object as originally constituted in response to the privacy preferences of the author of the content object or other restriction preferences being consistent with the content provider's policies (See e.g. [0033], 'To facilitate the requests... for data from Data Requesters, the system must provide several different functionalities, including the ability to... authorize release of data based on authorization rules and privacy policy matching and release data').

19. The method of claim 15 further comprising distributing any collected content object to a P3P servlet (See e.g. [0049], 'The Privacy Preference 302 specifies why and how the data can be accessed in terms of the P3P standards').

20. The method of claim 15, further comprising distributing any content object in response to the request to a privacy function (See e.g. [0030], 'This embodiment supports the enforcement of privacy preferences in data exchanges according to authorization checks based on the privacy preferences specified by a data subject with the privacy policies of a data requester' where the 'authorization checks' are considered 'privacy functions').

21. The method of claim 20, further comprising parsing the privacy preferences of an author of the content object or other restriction preferences (See e.g. [0033], 'the system must provide several different functionalities, including the ability to... authorize release of data based on authorization rules and privacy policy matching and release data').

23. A system for managing privacy preferences or access to restricted information, comprising:

a server to collect a content object in response to a request (See e.g. [0032], 'a Data Requester 105 can use a web browser 106 or some other computer programs 107 to send requests for data 109 as well as receive replies 110 to that request along with any returned data');

a privacy function operable on the server to access privacy preferences of an author of the content object or other restriction preferences (See e.g. [0033], 'the system must provide several different functionalities, including the ability to... define authorization rules and privacy controls'); and

means for comparing the privacy preferences or other restriction preferences to a content provider's policies (See e.g. [0033], 'the system must provide several different functionalities, including the ability to... authenticate requesters, authorize release of data based on authorization rules and privacy policy matching' where [0013], 'a data subject may want to setup privacy preference policies which can allow fully automatic release of data, even without knowing about the requester or the request itself... Similarly, a data subject may allow access to certain, non-identifiable financial data such as employment status and salary range, thus enabling interested financial institutions to automatically access such data and send solicitations for credit cards/loan requests to the data subjects' indicates that a 'requester' can also be a 'content provider').

24. The system of claim 23, wherein the privacy function distributes the content object as originally constituted in response to the privacy preferences or other restriction preferences being consistent with the content provider's policies (See e.g. [0033], 'To facilitate the requests... for data from Data Requesters, the system must provide several different functionalities, including the ability to... authorize release of data based on authorization rules and privacy policy matching and release data').

27. The system of claim 23, further comprising a collection function operable on the server to interrogate content sources and collect content objects from the content sources in responsive to the request (See e.g. [0032], 'a Data Requester 105 can use a web browser 106 or some other computer programs 107 to send requests for data 109 as well as receive replies 110 to that request along with any returned data' and Fig. 1).

32. A method of making a system for managing privacy preferences or access to restricted information, comprising:

providing a server to collect a content object in response to a request (See e.g. [0032], 'a Data Requester 105 can use a web browser 106 or some other computer programs 107 to send requests for data 109 as well as receive replies 110 to that request along with any returned data');

providing a privacy function operable on the server to access privacy preferences of an author of the content object or other restriction preferences (See e.g. [0033], 'the system must provide several different functionalities, including the ability to... define authorization rules and privacy controls'); and

providing means for comparing the privacy preferences or other restriction preferences to a content provider's policies (See e.g. [0033], 'the system must provide several different functionalities, including the ability to... authenticate requesters, authorize release of data based on authorization rules and privacy policy matching' where [0013], 'a data subject may want to setup privacy preference policies which can allow fully automatic release of data, even without knowing about the requester or the request itself... Similarly, a data subject may allow access to certain, non-identifiable financial data such as employment status and salary range, thus enabling interested financial institutions to automatically access such data and send solicitations for credit cards/loan requests to the data subjects' indicates that a 'requester' can also be a 'content provider').

33. The method of claim 32, further comprising adapting the privacy function to distribute the content object as originally constituted in response to the privacy preferences or other restriction preferences being consistent with the content provider's policies (See e.g. [0033], 'To facilitate the requests... for data from Data Requesters, the system must provide several different functionalities, including the ability to... authorize release of data based on authorization rules and privacy policy matching and release data').

35. The method of claim 32, further comprising providing a collection function to interrogate content sources and to collect content objects responsive to the request (See e.g. [0032], 'a Data Requester 105 can use a web browser 106 or some other computer programs 107

to send requests for data 109 as well as receive replies 110 to that request along with any returned data' and Fig. 1).

40. A computer-readable medium having computer executable instructions for performing a method, comprising:

collecting a content object responsive to a request (See e.g. [0032], 'a Data Requester 105 can use a web browser 106 or some other computer programs 107 to send requests for data 109 as well as receive replies 110 to that request along with any returned data');

accessing privacy preferences of an author of the content object or other restriction preferences (See e.g. [0033], 'the system must provide several different functionalities, including the ability to... define authorization rules and privacy controls'); and

comparing the privacy preferences or other restriction preferences to a content provider's policies (See e.g. [0033], 'the system must provide several different functionalities, including the ability to... authenticate requesters, authorize release of data based on authorization rules and privacy policy matching' where [0013], 'a data subject may want to setup privacy preference policies which can allow fully automatic release of data, even without knowing about the requester or the request itself... Similarly, a data subject may allow access to certain, non-identifiable financial data such as employment status and salary range, thus enabling interested financial institutions to automatically access such data and send solicitations for credit cards/loan requests to the data subjects' indicates that a 'requester' can also be a 'content provider').

41. The computer-readable medium having computer executable instructions for performing the method of claim 40, further comprising distributing the content object as originally constituted in response to the privacy preferences of the author of the content object or other restriction preferences being consistent with the content provider's policies (See e.g. [0033], 'To facilitate the requests... for data from Data Requesters, the system must provide several different functionalities, including the ability to... authorize release of data based on authorization rules and privacy policy matching and release data').

43. The computer-readable medium having computer executable instructions for performing the method of claim 40, further comprising distributing any content object responsive to the request to a privacy function (See e.g. [0030], 'This embodiment supports the enforcement of privacy preferences in data exchanges according to authorization checks based on the privacy preferences specified by a data subject with the privacy policies of a data requester' where the 'authorization checks' are considered 'privacy functions').

44. The computer-readable medium having computer executable instructions for performing the method of claim 43, further comprising parsing the privacy preferences of an author of the content object or other restriction preferences (See e.g. [0033], 'the system must provide several different functionalities, including the ability to... authorize release of data based on authorization rules and privacy policy matching and release data').

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3, 5, 7, 11, 18, 22, 28-30, 36-38, and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bohrer et al. as applied to claims 1, 2, 4, 6, 8-10, 12, 13, 15, 16, 19-21, 23, 24, 27, 32, 33, 35, 40, 41, 43, and 44 above, and further in view of Wikipedia.org's definitions of 'XLink', 'Java Servlet', and 'P3P'.

3. The method of claim 1, further comprising associating an xLink attribute to the restricted or personal information.

5. The method of claim 1, further comprising:
storing the restricted or personal information (See e.g. Bohrer et al. [0033], 'To facilitate the requests from a Data Subject to setup data profiles and privacy policies... The profiles are stored in a Profile Database 123 while the policies are stored in a Policy Database 124'); and
providing access to the restricted or personal information via one of an xLink or a secure connection.

7. The method of claim 6, wherein collecting any content objects responsive to the request comprises using a collection servlet.

11. The method of claim 10, further comprising locating or accessing privacy preferences of an author of the content object or other restriction preferences using an xLink.

18. The method of claim 15, further comprising using a collection servlet to collect the content object responsive to the request.

22. The method of claim 21, further comprising locating or accessing the privacy preferences or restriction preferences using an xLink.

28. The system of claim 23, wherein the privacy function comprises a P3P servlet to access the privacy preferences or other restriction preferences via an xLink.

29. The system of claim 28, wherein the P3P servlet comprises means for comparing the privacy preferences or other restriction preferences to a web site or content provider's policies (See e.g. Bohrer et al. [0003], 'In some cases the web site's privacy policy is compared to the consumer's policy preferences and warnings are issued when there is a mismatch').

30. The system of claim 29, wherein the P3P servlet comprises means for transmitting the content object as originally constituted to a collection servlet in response to the privacy preferences or restriction preferences being consistent with the web site or content provider's policies (See e.g. Bohrer et al. [0033], 'To facilitate the requests... for data from Data Requesters, the system must provide several different functionalities, including the ability to... authorize release of data based on authorization rules and privacy policy matching and release data').

36. The method of claim 32, further comprising providing a P3P servlet to access the privacy preferences or other restricted preferences via an xLink.

37. The method of claim 36, further comprising adapting the P3P servlet to compare the privacy preferences or other restriction preferences to a web site or content provider's policies (See e.g. Bohrer et al. [0003], 'In some cases the web site's privacy policy is compared to the consumer's policy preferences and warnings are issued when there is a mismatch').

38. The method of claim 37, further comprising adapting the P3P servlet to transmit the content object as originally constituted to a collection servlet in response to the privacy preferences or restriction preferences being consistent with the web site or content provider's policies (See e.g. Bohrer et al. [0033], 'To facilitate the requests... for data from Data Requesters, the system must provide several different functionalities, including the ability to... authorize release of data based on authorization rules and privacy policy matching and release data').

45. The computer-readable medium having computer executable instructions for performing the method of claim 44, further comprising locating or accessing the privacy preferences or restriction preferences using an xLink.

As per claims 3, 5, 7, 11, 18, 22, 28-30, 36-38, and 45, Wikipedia teaches:

Bohrer et al. do not disclose using xLinks, servlets, and P3P to access information, but Wikipedia discloses the motivation for doing so. Bohrer and Wikipedia are analogous art because they both discuss transferring data across a network. At the time of the invention, it would have been obvious to one of ordinary skill in the art to use xLinks, servlets, and P3P to access information over the Internet or other network.

As per xLinks, Wikipedia discloses that an xLink 'is an XML markup language used for creating hyperlinks for XML documents. XLink is a W3C specification which describes methods for allowing elements to be inserted into XML documents in order to create and describe links between resources, whether internal or external to the original document'.

As per servlets, Wikipedia discloses that using a servlet 'allows a software developer to add *dynamic* content to a Web server using the Java platform. The generated content is commonly HTML, but may be other data such as XML. Servlets are the Java counterpart to

dynamic web content technologies such as CGI, PHP or ASP. Servlets can maintain state across many server transactions by using HTTP cookies, session variables or URL rewriting'.

As per P3P, Wikipedia discloses that 'P3P is designed to give users a more precise control of the kind of information that they allow to release'.

Claims 14, 17, 25, 26, 34, and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bohrer et al. as applied to claims 1, 2, 4, 6, 8-10, 12, 13, 15, 16, 19-21, 23, 24, 27, 32, 33, 35, 40, 41, 43, and 44 above, and further in view of Fahlman et al., U.S. Pat. 5,960,080.

As per claims 14, 17, 25, 26, 34, and 42, Fahlman et al. teach:

14. The method of claim 12, further comprising:

deleting or replacing private or restricted information with default or generic information in response to the content privacy preferences of the author of the content object or other restriction preferences being inconsistent with the content provider's policies (See e.g. Brief Summary par. 14, 'transforming an original message into a final message by including an untrusted service includes... replacing the at least one sensitive term with a standard token to create a sanitized message' where 'an untrusted service' indicates a disparity in 'privacy' and 'restriction' preferences between the 'author' and 'provider');

repackaging the content object restriction preferences being inconsistent in response to deleting or replacing the private or restricted information (See e.g. Brief Summary par. 14, 'transforming an original message into a final message by... replacing the at least one sensitive term with a standard token to create a sanitized message'); and

distributing the repacked content object to a requester (See e.g. Brief Summary par. 14, 'transforming an original message into a final message by... transmitting the sanitized message to a provider of the untrusted service').

17. The method of claim 15, further comprising:

deleting or replacing private or restricted information with default or generic information in response to the privacy preferences of the author of the content object or other restriction preferences being inconsistent with the content provider's policies (See e.g. Brief Summary par. 14, 'transforming an original message into a final message by including an untrusted service includes... replacing the at least one sensitive term with a standard token to create a sanitized message' where 'an untrusted service' indicates a disparity in 'privacy' and 'restriction' preferences between the 'author' and 'provider');

repackaging the content object in response to deleting or replacing the private or restricted information (See e.g. Brief Summary par. 14, 'transforming an original message into a final message by... replacing the at least one sensitive term with a standard token to create a sanitized message'); and

distributing the repacked content object to a requester (See e.g. Brief Summary par. 14, 'transforming an original message into a final message by... transmitting the sanitized message to a provider of the untrusted service').

25. The system of claim 23, wherein the privacy function deletes or replaces private or restricted information with default or generic information in response to the privacy preferences or restriction preferences being inconsistent with the content provider's policies (See e.g. Brief Summary par. 14, 'transforming an original message into a final message by including an untrusted service includes... replacing the at least one sensitive term with a standard token to create a sanitized message' where 'an untrusted service' indicates a disparity in 'privacy' and 'restriction' preferences between the 'author' and 'provider').

26. The system of claim 25, wherein the privacy function repackages the content object in response to deleting or replacing the private or restricted information (See e.g. Brief Summary par. 14, 'transforming an original message into a final message by... replacing the at least one sensitive term with a standard token to create a sanitized message').

34. The method of claim 32, further comprising adapting the privacy function to delete or replace private or restricted information with default or generic information in response to the privacy preferences or restriction preferences being inconsistent with the content provider's policies (See e.g. Brief Summary par. 14, 'transforming an original message into a final message by including an untrusted service includes... replacing the at least one sensitive term with a standard token to create a sanitized message' where 'an untrusted service' indicates a disparity in 'privacy' and 'restriction' preferences between the 'author' and 'provider').

42. The computer-readable medium having computer executable instructions for performing the method of claim 40,

deleting or replacing private or restricted information with default or generic information in response to the privacy preferences of the author of the content object or other restriction preferences being inconsistent with the content provider's policies (See e.g. Brief Summary par. 14, 'transforming an original message into a final message by including an untrusted service includes... replacing the at least one sensitive term with a standard token to create a sanitized message' where 'an untrusted service' indicates a disparity in 'privacy' and 'restriction' preferences between the 'author' and 'provider');

repackaging the content object in response to deleting or replacing the private or restricted information (See e.g. Brief Summary par. 14, 'transforming an original message into a final message by... replacing the at least one sensitive term with a standard token to create a sanitized message'); and

distributing the repacked content object to a requester (See e.g. Brief Summary par. 14, 'transforming an original message into a final message by... transmitting the sanitized message to a provider of the untrusted service').

Bohrer et al. do not disclose replacing private information with generic language, but Fahlman et al. do make such a disclosure. Bohrer et al. and Fahlman et al. are analogous art because they both discuss transmitting messages with sensitive information in them. At the time of the invention, it would have been obvious to one of ordinary skill in the art to replace sensitive information in a transmission with generic information. The motivation is found in Fahlman et al. Brief Summary par. 9, 'even an automated service, such as an automatic grammar checker or

style checker, may create potential security leak under certain circumstances if the automated service has access to the full content of a message'.

Claims 31 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wikipedia as applied to claims 3, 5, 7, 11, 18, 22, 28-30, 36-38, and 45 above, and further in view of Fahlman et al., U.S. Pat. 5,960,080.

As per claims 31 and 39, Fahlman et al. teach:

31. The system of claim 30, wherein the P3P servlet comprises:

means for deleting or replacing private or restricted information with default or generic information in response to the privacy preferences or restriction preferences being inconsistent with the web site or content provider's policies (See e.g. Brief Summary par. 14, 'transforming an original message into a final message by including an untrusted service includes... replacing the at least one sensitive term with a standard token to create a sanitized message' where 'an untrusted service' indicates a disparity in 'privacy' and 'restriction' preferences between the 'author' and 'provider');

means for repackaging the content object in response to deleting or replacing the private or restricted information (See e.g. Brief Summary par. 14, 'transforming an original message into a final message by... replacing the at least one sensitive term with a standard token to create a sanitized message'); and

means for transmitting the repackaged content object to the collection servlet in response to the private or restricted information (See e.g. Brief Summary par. 14, 'transforming an original message into a final message by... transmitting the sanitized message to a provider of the untrusted service').

39. The method of claim 38, further comprising adapting the P3P sevlet to:

delete or replace private or restricted information with default or generic information in response to the privacy preferences or restriction preferences being inconsistent with the web site or content provider's policies (See e.g. Brief Summary par. 14, 'transforming an original message into a final message by including an untrusted service includes... replacing the at least one sensitive term with a standard token to create a sanitized message' where 'an untrusted service' indicates a disparity in 'privacy' and 'restriction' preferences between the 'author' and 'provider');

repackage the content object in response to deleting or replacing the private or restricted information (See e.g. Brief Summary par. 14, 'transforming an original message into a final message by... replacing the at least one sensitive term with a standard token to create a sanitized message'); and

transmit the repackaged content object to the collection sevlet in response to deleting or replacing the private or restricted information (See e.g. Brief Summary par. 14, 'transforming an original message into a final message by... transmitting the sanitized message to a provider of the untrusted service').

Wikipedia does not disclose replacing private information with generic language, but Fahlman et al. do make such a disclosure. Wikipedia and Fahlman et al. are analogous art because they both discuss transmitting messages with sensitive information in them. At the time of the invention, it would have been obvious to one of ordinary skill in the art to replace sensitive information in a transmission with generic information. The motivation is found in Fahlman et al. Brief Summary par. 9, 'even an automated service, such as an automatic grammar checker or style checker, may create potential security leak under certain circumstances if the automated service has access to the full content of a message'.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aaron J. Sanders whose telephone number is 571-270-1016. The examiner can normally be reached on M-Th 7:30a-5:00p.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David Bruce can be reached on 571-272-2487. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AJS

DAVID BRUCE
SUPERVISORY PATENT EXAMINER

AJS

PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	10/709,751
Filing Date	May 26, 2004
First Named Inventor	Fonda J. Daniels
Art Unit	2191
Examiner Name	Sanders
Attorney Docket Number	014682-000007

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
AJS	A	US-2004/0002878 A1		01/01/2004	Maria Hinton	
AJS	B	US-2003/0140230 A1		07/24/2003	de Jong et al.	
AJS	C	US-2003/0112791 A1		06/18/2003	Suryanarayana	
AJS	D	US-2003/0097383 A1		05/22/2003	Smirnov et al.	
AJS	E	US-2003/0088520 A1		05/08/2003	Bohrer, et al.	
AJS	F	US-2003/0014654 A1		01/16/2003	Adler, et al.	
AJS	G	US-2002/0104015 A1		08/01/2002	Barzilai, et al.	
AJS	H	US-6,578,046		06/10/2003	Chang et al.	
AJS	I	US-2003/0131058 A1		07/10/2003	Yaung	
AJS	J	US-2003/0041100 A1		02/27/2003	Nilsson, et al.	
AJS	K	US-2002/0124116 A1		09/05/2002	Yaung	
AJS	L	US-2002/0026443 A1		02/28/2002	Chang, et al.	
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]–Number[4]–Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

Examiner Signature	/Aaron Sanders/	Date Considered	07/26/2006

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional). 2 See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. 3 Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). 4 For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5 Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. 6 Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (08-03)
Approved for use through 08/30/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	10/709,751
				Filing Date	May 26, 2004
				First Named Inventor	Fonda J. Daniels
				Art Unit	2191
(use as many sheets as necessary)				Examiner Name	Sanders
Sheet	2	of	2	Attorney Docket Number	014682-000007

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
AJS	M	DOSS Document #: CA920030102US1 - Baek, OK.; Ewig S.C.; "Research Data Repository System and Method".	
AJS	N	Hull, R.; Kumar, B.; Lieuwen, D.; "Towards Federated Policy Management", Proceedings of the 4th International Workshop on Policies for Distributed Systems and Networks (POLICY '03)	
AJS	O	DOSS Document #: AUS920020412US1 – Hinton, H.; Blakley III, R.G.; Nadalin, A.; Pfitzmann, B.; "Method and System for Attribute Exchange in A Heterogeneous Federated Environment".	

Examiner Signature	/Aaron Sanders/	Date Considered	07/26/2006

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.
This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Notice of References Cited	Application/Control No. 10/709,751	Applicant(s)/Patent Under Reexamination DANIELS ET AL.	
	Examiner Aaron J. Sanders	Art Unit 2191	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,960,080 A	09-1999	Fahlman et al.	380/252
*	B	US-2003/0088520 A1	05-2003	Bohrer et al.	705/74
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
*	U	http://en.wikipedia.org/wiki/Xlink; accessed 7/25/2006
*	V	http://en.wikipedia.org/wiki/Servlet; accessed 7/25/2006
*	W	http://en.wikipedia.org/wiki/P3P; accessed 7/25/2006
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.